Cassandra Crossing/ Una chiave (USB) per la privacy

(21)— Basta una chiavetta USB per bypassare le misure di tecno-controllo. Una tutela per la propria privacy destinata a non piacere a chi…

Cassandra Crossing/ Una chiave (USB) per la privacy

Figure 1:

(21)— Basta una chiavetta USB per bypassare le misure di tecno-controllo. Una tutela per la propria privacy destinata a non piacere a chi auspica un monitoraggio continuato delle attività telematiche.

3 febbraio 2006—La storia dell'informatica è segnata da novità apparentemente piccole che hanno invece provocato grossi cambiamenti. Questo è vero sia per novità che hanno modificato la vita di tutti, anche di chi non le usa direttamente, come l'Intel 8008, Visicalc, il Pc IBM, il world wide web, sia per novità meno famose in settori più limitati, come Pgp in quello della privacy in Rete.

Per chi voleva difendere la privacy informatica, un piccolo programma come il grande Pgp ha permesso di misurarsi ad armi pari con chi aveva grandi mezzi per violarla, come la semi-mitica NSA.

Restando nel campo della privacy, un altro fenomeno recente, quello delle distribuzioni live di GNU/Linux, permette di creare un cd da usare su un computer qualsiasi.

Bootstrappando da cd e senza toccare l'hard disk del computer, evitando così eventuali trappole del suo sistema operativo, possiamo avere a disposizione un desktop GNU/Linux con tutte le applicazioni che ci servono, incluse quelle per la tutela della privacy.

Di recente è uscita una distribuzione Linux dedicata alla privacy, Anonym.OS Live CD che, pur con alcuni limiti di usabilità, probabilmente dettati dalla gioventù del progetto, procede nella direzione di rendere il desktop dell'utente contemporaneamente privato e facile da usare.

Linux, cd bootstrappabili, distribuzioni live non sono però adatti alla grande maggioranza di coloro che avrebbero bisogno, sempre di più, di tutelare la propria privacy in Rete. Il panorama dell'informatica di consumo non mostra infatti per ora significativi arretramenti (in percentuale) dei sistemi operativi proprietari, oltretutto sempre più lesivi della privacy.

Ma un nuovo "concetto", che è in realtà addirittura banale, promette di essere ancora più importante delle distribuzioni live, e sono le applicazioni entrocontenute.

Una applicazione entrocontenuta è una applicazione che è in grado di funzionare senza richiedere al sistema operativo nessuna risorsa tranne l'accesso al kernel; in termini un po' tecnici, non usa il caricamento dinamico di librerie o la memorizzazione di informazioni di configurazione e di file temporanei in risorse gestite dal sistema operativo.

In pratica tutta un'applicazione completamente configurata può trovarsi in un'unica directory, e quindi essere installata, spostata e rimossa come se fosse un semplice file, contrariamente alle normali applicazioni Unix, Windows ed ancora meglio di quelle MacOS.

Esiste una interessante applicazione entrocontenuta per l'ambiente windows, TorPark che unisce il browser Mozilla Firefox standalone ad una rete anonimizzante come Tor: è sufficiente copiarla in una chiave USB da pochi mega per portarsi in giro il proprio ambiente di navigazione privata ed usarlo su qualunque computer che abbia un sistema operativo Windows.

Basta inserire la chiavetta, aspettare che venga vista dal sistema operativo, lanciare l'applicativo Torpark e dargli qualche secondo di tempo per aprire i circuiti. Ed è possibile navigare in maniera protetta, salvare i propri file e mettere bookmark senza lasciare tracce sul computer ospitante. Nessuna configurazione o decisione da prendere. Nessuna necessità di salvare informazioni altrove.

Alla fine della navigazione basta lanciare l'applicazione Torkill.exe, aspettare qualche secondo e rimettersi in tasca la chiave. Tutto qui. Per chi ha passato tanto tempo configurando e riconfigurando questi applicativi ogni volta che cambiava computer è praticamene un sogno.

Certo, anche Torpark non offre garanzie assolute; se protegge dalle violazioni della privacy effettuate tramite la Rete non protegge ad esempio da quelle realizzate tramite un keylogger sul computer ospitante. Se il vostro nemico è potente e ce l'ha proprio con voi non serve, ma per non essere vittime del tecnocontrollo e della data retention, è perfetto.

L'obiettivo trainante di TorPark infatti non è di proteggere l'utente dalla NSA, ma piuttosto dai tentativi di tecnocontrollo, fatti passare come misure antiterrorismo, come quelli a cui sono oggi obbligati gli Internet Cafè.

Non c'è identificazione obbligatoria dell'utente che tenga se poi diventa possibile anonimizzarsi anche in un ambiente controllato.

Potremmo chiamare le distribuzioni live e le applicazioni entrocontenute come le prime parti di un "Pacchetto Privacy" da opporre ad un ben più famoso pacchetto che da diversi mesi sta facendo polpette della privacy degli italiani, coniugando controlli di identità obbligatori con data retention senza limiti temporali.Una nota per terminare, valida non solo in questo caso ma per tutte le risorse dedicate alla privacy. Non esistono cose come i pasti gratis. Lo sviluppo di Tor, TorPark, Privoxy e compagnia cantando è fatto su base volontaria da pochi individui che donano il loro tempo alla comunità, senza ricavarne nulla, con tanti oneri ed al massimo pochi onori.

Soldi zero.

Usare la rete Tor significa usare software sviluppato da volontari e costosa banda condivisa da altri individui che, pur non potendo programmare, ritengono il progetto Tor così importante da gestire i router Tor e donargli una parte della banda delle loro ADSL. Se, come è auspicabile, Tor prenderà piede, rischierà subito di restare vittima del suo successo a meno che chi lo usa non contribuisca in qualche modo al suo funzionamento.

Se potete, create un router Tor; se non potete perché con l'informatica e le reti non andate tanto d'accordo, levatevi di tasca qualche spicciolo e finanziate il progetto Tor e gli altri suoi simili (Freenet, Mixminion….).

EFF infatti ha potuto finanziare solo per 12 mesi il progetto Tor, che da gennaio è nuovamente senza nessun finanziamento.

Qui trovate le indicazioni su come inviare contributi; se non avete direttamente la possibilità di farlo, perché ad esempio non avete un account PayPal, fatelo via banca, anche se è noioso, o fatelo fare ad un amico con l'account PayPal. Potete anche chiedere, sulle liste che trattano di questioni come e-privacy o cyberrights, l'aiuto di chi ne è dotato.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on December 9, 2023.

Canonical link

Exported from Medium on August 27, 2025.